ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Algebra 300 (2005) 35–43

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Transfer kernels for finite groups ☆

K.W. Gruenberg [a], A. Weiss [b]

[a] School of Mathematical Sciences, Queen Mary, University of London, Mile End Road, London E1 4NS, UK

[b] Department of Mathematical Sciences, University of Alberta, Edmonton, Alberta, Canada, T6G 2G1

Received 28 July 2005

Available online 10 January 2006

Communicated by Derek Holt

To Charles Leedham-Green for his 65th birthday and to celebrate a long friendship

Given a finite group G, we are concerned here with the class $\mathfrak{X}(G)$ of all finite abelian groups X of the form $H^0(G,S)$ (Tate cohomology), where S is a $\mathbb{Z}G$-lattice whose rational character is regular plus trivial ($\mathbb{Q}S \simeq \mathbb{Q}G^{(r)} \oplus \mathbb{Q}$ for some $r \geqslant 0$). In view of the structural complexity of lattices over finite groups, it is surprising that nevertheless general statements about $\mathfrak{X}(G)$ are possible. Indeed, we reduce the problem to the case of prime-power groups where interesting questions remain, the most basic of which are apparently of a computational nature.

The significance of $\mathfrak{X}(G)$ comes from the capitulation problem of class field theory ([5,7], [2]). If K/k is a finite, unramified Galois extension of algebraic number fields with Galois group G and $c: Cl_k \to Cl_K$ is the capitulation homomorphism of the respective ideal class groups, then the kernel of c is in $\mathfrak{X}(G)$. The transition to group theory discovered by Artin [1] shows that the kernel of c is a *transfer kernel* for G in the language of [2, §1]. From this the identification of the class of transfer kernels for G with the class $\mathfrak{X}(G)$ follows easily: one direction is part of the proof of Theorem 2, (a) ⇒ (b) of [2, §2], while the converse is (2.3) in [3].

Note that, since the groups in $\mathfrak{X}(G)$ are cohomology groups, every X in $\mathfrak{X}(G)$ satisfies $|G|X = 0$. We say X in $\mathfrak{X}(G)$ is *minimal* if no proper quotient of X is in $\mathfrak{X}(G)$ and shall denote the class of minimal objects in $\mathfrak{X}(G)$ by $\min \mathfrak{X}(G)$. As usual, $O^p(G)$ is the smallest normal subgroup of G with quotient a p-group. We collect the main facts in

☆ The authors gratefully acknowledge financial help from EPSRC and NSERC.

E-mail addresses: k.w.gruenberg@qmul.ac.uk (K.W. Gruenberg), weissa@ualberta.ca (A. Weiss).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.11.030

Theorem A.

(i) $\mathfrak{X}(G)$ *consists of all* $\mathbb{Z}/|G|\mathbb{Z}$*-modules that have a homomorphic image in* $\min \mathfrak{X}(G)$;
(ii) $\min \mathfrak{X}(G) = \prod_{p/|G|} \min \mathfrak{X}(G/O^p(G))$;
(iii) *for every* X *in* $\min \mathfrak{X}(G)$, $|G/[G,G]|$ *divides* $|X|$ *and* $|X|$ *divides* $|G|$.

Part (iii) gives a universal upper bound and a universal lower bound for the orders of minimal transfer kernels of G. But establishing these bounds involves quite different ideas. The upper bound $|G|$ comes from the fact that $\mathfrak{X}(G)$ contains every abelian group of order $|G|$ (Proposition 4); while the lower bound $|G/[G,G]|$ is proved by a classical determinantal argument derived from [4], the germ of the concept of Fitting ideal. Of course, the existence of the upper bound shows that $\min \mathfrak{X}(G)$ *is finite for every* G. When G is abelian, parts (iii) and (i) together with Proposition 4 regains the main result of [2].

Part (ii) effectively reduces the study of $\min \mathfrak{X}(G)$ to that of prime power groups. Moreover the result can be rephrased thus: $\min \mathfrak{X}(G) = \min \mathfrak{X}(G/C)$, *where* C *is the limit of the lower central series of* G.

All the arguments here depend on another characterization of transfer kernels. This is given in Theorem 1, which is essentially Theorem 2 of [2]. But our proof here is more transparent than our earlier one, primarily because we are able to use some simple general facts about module extensions that we developed for [3], and which are explained in Section 1 of that paper. Other ideas implicit in [2] will occur; making them explicit has uncovered the role of the lattices on the augmentation space.

Theorem 1 is proved in Section 1, as is part (i) of Theorem A. In Section 2 we discuss three methods of constructing transfer kernels—from G to image groups, from group extensions to G and from p-primary components. We can then prove the remaining parts of Theorem A: part (ii) at the beginning of Section 3 and part (iii) at the end. In the final Section 4 we turn to p-groups, giving examples and discussing computational issues. We hope that computational experience with $\mathfrak{X}_p(G)$ will lead to new constructions and new bounds.

1. The augmentation space

We write ΔG for the augmentation ideal of $\mathbb{Z}G$ and $\hat{G} = \sum_{g\in G} g$. If M is a $\mathbb{Z}G$-module, the set of G-invariants is $M^G = \{x \in M \mid gx = x \text{ for all } g \in G\}$, whence $H^0(G,M) = M^G/\hat{G}M$. The set of G-coinvariants is $M_G = M/(\Delta G)M$, and $H^{-1}(G,M) = (\text{ker of } \hat{G} \text{ on } M)/(\Delta G)M$. We set $\Lambda = \mathbb{Z}G/\hat{G}\mathbb{Z}$ and note that Λ is a ring. Then $\mathbb{Q}\Lambda = \mathbb{Q}\Delta G$ and the $\mathbb{Z}G$-module M is a Λ-module if, and only if, $\hat{G}M = 0$. For such a module, $M_G = H^{-1}(G,M)$.

The significance of the augmentation space $\mathbb{Q}\Lambda$ is embodied in the following characterization of transfer kernels:

Theorem 1. *X is a transfer kernel for G if, and only if, there exists a finitely generated Λ-module M such that $X \simeq M_G$ and $\mathbb{Q}M \simeq \mathbb{Q}\Lambda$.*

Proof. If X is a transfer kernel for G, choose S so that $X \simeq H^0(G,S)$. Writing $T = S^G$ and $U = S/T$, we obtain an extension $T \hookrightarrow S \twoheadrightarrow U$ of G-modules. Note that U is a lattice and $T \simeq \mathbb{Z}^{(m)}$ because $\mathbb{Q}S \simeq \mathbb{Q}G^{(m-1)} \oplus \mathbb{Q}$ for some $m \geqslant 1$.

Applying $\mathrm{Hom}(U,-)$ to $T \hookrightarrow S \twoheadrightarrow U$ produces a new exact sequence of G-modules. In the resulting cohomology sequence we take the connecting homomorphism

$$H^0\big(G, \mathrm{Hom}(U,U)\big) \to H^1\big(G, \mathrm{Hom}(U,T)\big)$$

and follow it with the natural isomorphism $H^1(G, \mathrm{Hom}(U,T)) \xrightarrow{\sim} \mathrm{Ext}^1_G(U,T)$. This gives a homomorphism $\delta_S : \mathrm{Hom}_G(U,U) \to \mathrm{Ext}^1_G(U,T)$. The theory of module extensions ensures that the extension class of S is the image of id_U.

Now T also fits into an exact G-sequence $T \rightarrowtail \mathbb{Z}G^{(m)} \twoheadrightarrow \Lambda^{(m)}$. Again we apply $\mathrm{Hom}(U,-)$ and take the resulting cohomology sequence. Here all the connecting homomorphisms are isomorphisms since $\mathrm{Hom}(U, \mathbb{Z}G)$ is cohomologically trivial. Thus

$$H^0\big(G, \mathrm{Hom}\big(U, \Lambda^{(m)}\big)\big) \xrightarrow{\sim} \mathrm{Ext}^1_G(U,T)$$

and so the extension class of S is $[\beta]$ for some $\beta \in \mathrm{Hom}_G(U, \Lambda^{(m)})$. We claim that the pull-back of $T \rightarrowtail \mathbb{Z}G^{(m)} \twoheadrightarrow \Lambda^{(m)}$ along β determines the extension class of our S. The short argument for this (cf. [3, 1.1]) runs as follows: The pull-back diagram

$$\begin{tikzcd}
T \arrow[r, tail] \arrow[d, equal] & S' \arrow[r, two heads] \arrow[d] & U \arrow[d, "\beta"] \\
T \arrow[r, tail] & \mathbb{Z}G^{(m)} \arrow[r, two heads] & \Lambda^{(m)}
\end{tikzcd}$$

produces

$$\begin{tikzcd}
\mathrm{Hom}_G(U,U) \arrow[r, "\delta_{S'}"] \arrow[d, "\beta_*"'] & \mathrm{Ext}^1_G(U,T) \arrow[d, equal] \\
\mathrm{Hom}_G(U, \Lambda^{(m)}) \arrow[r, "\delta_{\mathbb{Z}G^{(m)}}"'] & \mathrm{Ext}^1_G(U,T)
\end{tikzcd}$$

which gives $\delta_{S'}(\mathrm{id}_U) = \delta_{\mathbb{Z}G^{(m)}}(\beta)$, where the left side is the extension class of S' and the right side is the extension class of S.

Now $\mathbb{Q}U \simeq \mathbb{Q}\Lambda^{(m-1)} \hookrightarrow \mathbb{Q}\Lambda^{(m)}$. As a consequence there exists a monomorphism $\alpha : U \rightarrowtail \Lambda^{(m)}$ such that $[\alpha] = [\beta]$: for the proof of this fact we refer to the last paragraph of the proof of 1.3 in [3]. Thus S is also the pull-back along α. Writing M for the cokernel of α, we have the following diagram:

$$\begin{tikzcd}
T \arrow[r, tail] \arrow[d, equal] & S \arrow[r, two heads] \arrow[d, tail] & U \arrow[d, tail, "\alpha"] \\
T \arrow[r, tail] & \mathbb{Z}G^{(m)} \arrow[r, two heads] \arrow[d, two heads] & \Lambda^{(m)} \arrow[d, two heads] \\
 & M \arrow[r, equal] & M
\end{tikzcd}$$

It is now clear that M is the required Λ-module: From the middle column in the diagram, $M_G = H^{-1}(G, M) \simeq H^0(G, S) \simeq X$; and from the right-hand column, $\mathbb{Q}\Lambda^{(m)} \simeq \mathbb{Q}M \oplus \mathbb{Q}U \simeq \mathbb{Q}M \oplus \mathbb{Q}\Lambda^{(m-1)}$.

The converse is trivial: If $X = M_G$, take a free presentation $S \rightarrowtail \mathbb{Z}G^{(m)} \twoheadrightarrow M$. Then we have $H^0(G, S) \simeq H^{-1}(G, M) = M_G$ and $\mathbb{Q}M \oplus \mathbb{Q}S \simeq \mathbb{Q}G^{(m)}$. $\square$

Proof of Theorem A(i). Let $Y \hookrightarrow X \twoheadrightarrow X'$ be an exact sequence of finite abelian groups with $|G|X = 0$. We view the sequence as one of Λ-modules (trivial $\mathbb{Z}G$-modules killed by $\hat{G}$). Assume X' is a transfer kernel for G. We must prove the same for X.

By Theorem 1, $X' = M'_G$ with suitable M'. Taking the pull-back of the extension X along $M' \twoheadrightarrow X'$ gives the diagram

$$\begin{tikzcd}
 & N \arrow[r, equal] \arrow[d, tail] & N \arrow[d, tail] \\
Y \arrow[r, tail] \arrow[d, equal] & M \arrow[r, two heads] \arrow[d, two heads] & M' \arrow[d, two heads] \\
Y \arrow[r, tail] & X \arrow[r, two heads] & X'
\end{tikzcd}$$

Here M is a Λ-module since both X and M' are. The middle row implies M is finitely generated with $\mathbb{Q}M \simeq \mathbb{Q}\Lambda$. So it remains to prove $M_G \simeq X$. Taking G-coinvariants of our diagram gives

$$\begin{tikzcd}
 & N_G \arrow[r, equal] \arrow[d] & N_G \arrow[d, "0"] \\
Y \arrow[r] \arrow[d, equal] & M_G \arrow[r, two heads] \arrow[d, two heads] & M'_G \arrow[d, two heads] \\
Y \arrow[r, tail] & X \arrow[r, two heads] & X'
\end{tikzcd}$$

where $N_G \to M'_G$ is the zero map because $M'_G = X'$. A direct diagram chase now shows $N_G \to M_G$ is also zero. $\square$

Theorem 1 ensures that every X in $\min \mathfrak{X}(G)$ has the form L_G for some (full) $\mathbb{Z}G$-lattice on the augmentation space $\mathbb{Q}\Lambda$: for X has the form M_G for a suitable M and so, if $L = M/T$ (T the $\mathbb{Z}$-torsion of M), then $X \twoheadrightarrow L_G$, whence $X \xrightarrow{\sim} L_G$ by minimality. The Jordan–Zassenhaus Theorem shows that there exist only finitely many (isomorphism classes of) Λ-lattices with rational character $\mathbb{Q}\Lambda$. This proves $\min \mathfrak{X}(G)$ is finite; but we regain this fact later (via Theorem A(iii)) without the use of Jordan–Zassenhaus.

2. Constructions

Our *first* construction starts with a transfer kernel for G and produces one for an image group:

Proposition 1. *Let N be a normal subgroup of G and set $\bar{G} = G/N$. If X is a transfer kernel for G, then $X/|\bar{G}|X$ is a transfer kernel for $\bar{G}$.*

Proof. By Theorem 1, $X = M_G$ for a G-module M satisfying $\hat{G}M = 0$ and $\mathbb{Q}M = \mathbb{Q}\Delta G$. We set $\bar{M} = M_N/\hat{\bar{G}}M_N$. Then $\bar{M}$ is a $\bar{G}$-module that satisfies $\hat{\bar{G}}\bar{M} = 0$; also $\mathbb{Q}\bar{M} \simeq \mathbb{Q}M_N$ (because $|N|\hat{\bar{G}}M_N = \hat{G}M_N = 0$) and $\mathbb{Q}M_N \simeq \mathbb{Q}(\Delta G)_N \simeq \mathbb{Q}\Delta\bar{G}$ (because the group extension $N \hookrightarrow G \twoheadrightarrow \bar{G}$ provides the $\bar{G}$-module extension $N/[N,N] \rightarrowtail (\Delta G)_N \twoheadrightarrow \Delta\bar{G}$: e.g., [2, §1]). Finally,

$$\bar{M}_{\bar{G}} = M_N/\big(\hat{\bar{G}}M_N + (\Delta\bar{G})M_N\big) = M_N/\big(|\bar{G}|M_N + (\Delta\bar{G})M_N\big) = M_G/|\bar{G}|M_G. \qquad \square$$

The *second* construction makes transfer kernels from normal subgroups and quotient groups.

Proposition 2. *Let N be a normal subgroup of G and set $\bar{G} = G/N$. If X' is in $\mathfrak{X}(N)$ and X'' is in $\mathfrak{X}(\bar{G})$, then $X' \oplus X''$ is in $\mathfrak{X}(G)$.*

Proof. We know $X' = M'_N$ for a suitable N-module M' and $X'' = M''_{\bar{G}}$ for a suitable $\bar{G}$-module M''. Let $M = \operatorname{ind}_N^G M' \oplus M''$ with G acting on M'' by $G \to \bar{G}$. Then $\hat{G}M = 0$ and this implies $M_G = H^{-1}(G, M)$ (recall that we use Tate cohomology exclusively), whence using Shapiro's Lemma,

$$M_G = H^{-1}(N, M') \oplus H^{-1}(G, M'') = M'_N \oplus M''_G = X' \oplus X''.$$

Finally, $\mathbb{Q}M \simeq \mathbb{Q}\Delta G$ follows from $\operatorname{ind}_N^G \Delta N \hookrightarrow \Delta G \twoheadrightarrow \Delta\bar{G}$. $\square$

A *third* method of constructing transfer kernels is to proceed one prime at a time. If A is an abelian group, let $A(p)$ denote its p-primary component. For a $\mathbb{Z}G$-module M, set

$M_{(p)} = \mathbb{Z}_{(p)} \otimes M$ (where $\mathbb{Z}_{(p)}$ is the local ring at p). Define $\mathfrak{X}_p(G) = \{X(p) \mid X \text{ in } \mathfrak{X}(G)\}$. The usefulness of separating the primes comes from Proposition 3 below. To prepare for this we need

Lemma 1. *For each prime p dividing $|G|$, let M_p be a $\Lambda_{(p)}$-module such that $\mathbb{Q}M_p \simeq \mathbb{Q}\Lambda$. Then there exists a Λ-module M such that $\mathbb{Q}M \simeq \mathbb{Q}\Lambda$ and $M_{(p)} \simeq M_p$ for all p.*

Proof. Let T_p be the $\mathbb{Z}_{(p)}$-torsion in M_p and $L_p \simeq M_p/T_p$ with $L_p \subseteq \mathbb{Q}\Lambda$. By [6, 4.22] there exists a Λ-lattice L on $\mathbb{Q}\Lambda$ with $L_{(p)} = L_p$, for every p dividing $|G|$ (note that G acts on the lattice constructed in [6] and that primes p that do not divide $|G|$ can be accommodated by taking $L_p = \Lambda_{(p)}$; Λ plays the role of M in the proof given in [6]).

If $T = \bigoplus_{p/|G|} T_p$, then $T_{(p)} = T_p$ for all p dividing $|G|$ and we have the exact sequences $T_{(p)} \rightarrowtail M_p \twoheadrightarrow L_{(p)}$. These together provide an element in the right-hand side of

$$\operatorname{Ext}^1_{\mathbb{Z}G}(L, T) \simeq \bigoplus_{p/|G|} \operatorname{Ext}^1_{\mathbb{Z}_{(p)}G}(L_{(p)}, T_{(p)}).$$

The element corresponding to this in the left-hand side is an extension $T \hookrightarrow M \twoheadrightarrow L$, which gives the required M. $\square$

The following is a p-version of Theorem 1:

Theorem 1p. *X is in $\mathfrak{X}_p(G)$ if, and only if, there exists a finitely generated $\Lambda_{(p)}$-module M so that $X \simeq M_G$ and $\mathbb{Q}M \simeq \mathbb{Q}\Lambda_{(p)}$.*

This is immediate: If X is in $\mathfrak{X}_p(G)$, then $X = Y(p)$ for some Y in $\mathfrak{X}(G)$. By Theorem 1, $Y = M'_G$ for some Λ-module M' with $\mathbb{Q}M' \simeq \mathbb{Q}\Lambda$. Then $M'_{(p)}$ will do for M as $(M'_{(p)})_G = (M'_G)_{(p)}$. Conversely, if M is a $\Lambda_{(p)}$-module with $\mathbb{Q}M \simeq \mathbb{Q}\Lambda_{(p)}$, Lemma 1 gives a Λ-module M' so that $M \simeq M'_{(p)}$, whence $X = M'_G(p)$ is in $\mathfrak{X}_p(G)$ by Theorem 1. $\square$

We also obtain p-versions of Propositions 1 and 2 by simply replacing $\mathbb{Z}$ by $\mathbb{Z}_{(p)}$ and Theorem 1 by Theorem 1p in the statements and proofs:

Proposition 1p. *If $\bar{G} = G/N$ and X is in $\mathfrak{X}_p(G)$, then $X/|\bar{G}|X$ is in $\mathfrak{X}_p(\bar{G})$.*

Proposition 2p. *If $\bar{G} = G/N$ and X' is in $\mathfrak{X}_p(N)$, X'' in $\mathfrak{X}_p(\bar{G})$, then $X' \oplus X''$ is in $\mathfrak{X}_p(G)$.*

We are now ready for the basic

Proposition 3.

(i) $\mathfrak{X}(G) \xrightarrow{\sim} \prod_{p/|G|} \mathfrak{X}_p(G)$ *and this induces*;
(ii) $\min \mathfrak{X}(G) \xrightarrow{\sim} \prod_{p/|G|} \min \mathfrak{X}_p(G)$.

Proof. (i) The map sending X to the tuple $(X(p))_p$ in $\prod \mathfrak{X}_p(G)$ is clearly injective. To see it is surjective, take $((M_p)_G)_p$ in $\prod \mathfrak{X}_p(G)$, where M_p is a $\Lambda_{(p)}$-module with $\mathbb{Q}M_p \simeq \mathbb{Q}\Lambda$. Lemma 1 provides a Λ-module M such that $M_G(p) = (M_p)_G$ for all relevant primes p.

(ii) Let X be in $\min \mathfrak{X}(G)$ and suppose $X(p) \twoheadrightarrow Y(p)$ for some transfer kernel Y of G. The bijection of (i) enables us to find a transfer kernel X' of G such that $X'(p) = Y(p)$, $X'(q) = X(q)$ for all $q \neq p$. Then $X \twoheadrightarrow X'$ and this shows $X \xrightarrow{\sim} X'$ by the minimality of X, whence $X(p) \xrightarrow{\sim} Y(p)$. So $X(p) \in \min \mathfrak{X}_p(G)$. The converse is clear. □

3. Minimal transfer kernels

Proof of Theorem A(ii). We begin by showing $\mathfrak{X}_p(G/O^p(G)) \subseteq \mathfrak{X}_p(G)$. Now $N = O^p(G)$ has $N/[N,N]$ a p'-group, so $M = (\Delta N)_{(p)}$ has $M_N = (N/[N,N])_{(p)} = 0$ and Theorem 1p implies that 0 is in $\mathfrak{X}_p(N)$. Then Proposition 2p gives $\mathfrak{X}_p(G/N) \subseteq \mathfrak{X}_p(G)$. Theorem A(ii) now follows from Proposition 3(ii) and

Lemma 2. *If N is a normal subgroup of G, then $\mathfrak{X}_p(G/N) \subseteq \mathfrak{X}_p(G)$ implies* $\min \mathfrak{X}_p(G/N) = \min \mathfrak{X}_p(G)$.

Proof. Set $\bar{G} = G/N$. If $X \in \min \mathfrak{X}_p(G)$ then $\bar{X} = X/|\bar{G}|X$ is in $\mathfrak{X}_p(\bar{G})$ (by Proposition 1p) Now $\bar{X} \twoheadrightarrow X'$ for some X' in $\min \mathfrak{X}_p(\bar{G})$. Since X' is in $\mathfrak{X}_p(G)$, by hypothesis, the composite $X \twoheadrightarrow \bar{X} \twoheadrightarrow X'$ must be an isomorphism by the minimality of X in $\mathfrak{X}_p(G)$. Thus $X \xrightarrow{\sim} X'$ gives X in $\min \mathfrak{X}_p(\bar{G})$. The opposite inclusion is similar. □

Proposition 4. $\mathfrak{X}(G)$ *contains all abelian groups of order* $|G|$.

Proof. By parts (i) and (ii) of Theorem A, it suffices to prove the proposition for $G/O^p(G)$. Change notation and let G be a p-group. We use induction on $|G|$.

If A is an abelian group of order $|G|$ then $|G|A = 0$ and this implies $A = A' \oplus \mathbb{Z}/p^s\mathbb{Z}$ for some p^s dividing $|G|$. Since G is a p-group, there exists a normal subgroup N of index p^s giving $|N| = |A'|$. Set $\bar{G} = G/N$. By induction A' is in $\mathfrak{X}(N)$ and $\mathbb{Z}/p^s\mathbb{Z} = \bar{\Lambda}_{\bar{G}}$ is in $\mathfrak{X}(\bar{G})$, by Theorem 1. Proposition 2 completes the induction. □

Proof of Theorem A(iii). Let X be in $\min \mathfrak{X}(G)$. If p divides $|G|$, Theorem A(ii) implies that $X(p)$ is in $\min \mathfrak{X}(G/O^p(G))$, hence $|X(p)|$ divides $|G/O^p(G)|$ by Proposition 4. Then $|X| = \prod_p |X(p)|$ divides $\prod_p |G/O^p(G)|$, which divides $|G|$.

It remains to prove that $G/[G,G]$ has order dividing every $|X|$. Write $\bar{G} = G/[G,G]$ and use Proposition 1 to construct the transfer kernel $\bar{X} = X/|\bar{G}|X$ for $\bar{G}$. The classical determinant argument (as repeated in [2, §3], (ii) $\Rightarrow$ (i)) shows $|\bar{G}|$ divides $|\bar{X}|$, whence $|\bar{G}|$ also divides $|X|$. □

Corollary. $G/[G,G]$ *is in* $\min \mathfrak{X}(G)$.

Proof. Since $G/[G,G] \simeq (\Delta G)_G$ is a transfer kernel for G by Theorem 1, its minimality follows from Theorem A(iii). □

4. p-Groups

Choose a prime p and assume from now on that G is a p-group. Then $\mathfrak{X}(G) = \mathfrak{X}_p(G)$.

Lemma 3. *If $X = M_G$ with M a finitely generated $\Lambda_{(p)}$-module, then the minimum number of generators of M as $\Lambda_{(p)}$-module equals the minimum number of generators of X as abelian group.*

Proof. Since $\operatorname{rad}\mathbb{Z}_{(p)}G = p\mathbb{Z}_{(p)}G + (\Delta G)_{(p)}$, we have $M/(\operatorname{rad}\mathbb{Z}_{(p)}G)M \simeq X/pX$ and now Nakayama's Lemma finishes the proof. □

We collect some simple observations in

Proposition 5. *Suppose $|G| = p^n$.*

(a) $\mathbb{Z}/|G|\mathbb{Z}$ *is in* $\min\mathfrak{X}(G)$;
(b) $\min\mathfrak{X}(G)$ *contains only one elementary abelian p-group*; *its rank $m(G)$ is $\leqslant n$*;
(c) *every X in* $\min\mathfrak{X}(G)$ *with $pX \neq 0$ has $< m(G)$ generators.*

Proof. (a) Suppose X is cyclic and in $\mathfrak{X}(G)$. Then $X = M_G$ for a suitable $\Lambda_{(p)}$-module M as in Theorem 1p. By Lemma 3 there is a $\Lambda_{(p)}$-module epimorphism $\Lambda_{(p)} \twoheadrightarrow M$. This is an isomorphism because $\mathbb{Q}\Lambda_{(p)} \simeq \mathbb{Q}M$, whence $X \simeq (\Lambda_{(p)})_G = \mathbb{Z}/|G|\mathbb{Z}$.

(b) $\mathfrak{X}(G)$ contains an elementary abelian p-group of rank n by Proposition 4, hence $\min\mathfrak{X}(G)$ has one of rank $m \leqslant n$. This rank m is unique by minimality.

(c) If X in $\mathfrak{X}(G)$ has $\geqslant m$ generators, then X maps onto an elementary abelian group X' on $m(G)$ generators. If X were minimal we would have $X \xrightarrow{\sim} X'$, contradicting $pX \neq 0$. □

We finally illustrate the ambiguities presently left in our understanding of $\min\mathfrak{X}(G)$ by constructing the simplest examples. Our tools will be Theorem A(iii) and its Corollary (at end of Section 3), Propositions 4 and 5. We also find it useful to denote the isomorphism type of a finite abelian p-group A by the sequence of exponents of p in the orders of the invariant factors of A, taken in *decreasing* order, and followed by infinitely many zeros (which are understood when not written). This has the merit that A of type $(a_r)_r$ maps onto A' of type $(a'_r)_r$ if, and only if, $a_r \geqslant a'_r$ for all r.

Example 1. *G of order p^3.* If G is abelian, then by [2], $\min\mathfrak{X}(G) = \{(3), (2,1), (1,1,1)\}$ with the obvious abuse of notation. If G is nonabelian, then $G/[G,G]$, being noncyclic, has type $(1,1)$. By our tools, $\mathfrak{X}(G)$ contains (3), $(2,1)$, $(1,1,1)$, $(1,1)$, with first and last minimal; and our bounds admit no other type. Thus $\min\mathfrak{X}(G) = \{(3), (1,1)\}$.

Example 2. *G nonabelian of order p^4.* There are three possibilities for the type of $G/[G,G]$:

(a) $(1,1)$. Here $\min\mathfrak{X}(G) = \{(4), (1,1)\}$, as in Example 1.

(b) $(2, 1)$. In this case $\mathfrak{X}(G)$ contains the following groups with first and last minimal: $(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1), (2, 1)$; and our bounds permit only possibly $(1, 1, 1)$ in addition. So $\min \mathfrak{X}(G)$ is $\{(4), (2, 1), (1, 1, 1)\}$ if $(1, 1, 1)$ is in $\mathfrak{X}(G)$, and $\{(4), (2, 1), (1, 1, 1, 1)\}$ if not.

(c) $(1, 1, 1)$. As in (b), $\min \mathfrak{X}(G) = \{(4), (2, 1), (1, 1, 1)\}$ if $(2, 1)$ is in $\mathfrak{X}(G)$, but if $(2, 1)$ is not in $\mathfrak{X}(G)$, then $\min \mathfrak{X}(G) = \{(4), (3, 1), (2, 2), (1, 1, 1)\}$.

Although our constructions, as above, show that $\min \mathfrak{X}(G)$ is not enormous, the basic problem is still that we have no simple method (except using the lower bound of Theorem A(iii), which has limited scope) of proving that a finite abelian group A is *not* in $\mathfrak{X}(G)$. The only available general method for determining $\mathfrak{X}(G)$ is that of the last paragraph of Section 1: survey all (isomorphism classes of) Λ-lattices L on $\mathbb{Q}\Lambda$ and compute L_G for each. The Jordan–Zassenhaus Theorem is a necessary condition for this to be possible, but already computationally unwieldy because there are normally very many lattices, even within a single genus. Of course there remains the serious problem of deciding when such a survey is complete.

Proposition 5 suggests that one should survey $\Lambda_{(p)}$-lattices on $\mathbb{Q}\Lambda_{(p)}$. More precisely, if d is "small" for G, survey the $\Lambda_{(p)}$-lattices L on $\mathbb{Q}\Lambda_{(p)}$ with $< d$ generators; note that Lemma 3 finds the number of generators of L in a way that fits well into our problem. We do not know whether existing (or potential) algorithms take advantage of the "smallness" of d in a useful way.

But if one has such an algorithm, then $\min \mathfrak{X}_p(G)$ may be determined as follows, using the notation of Proposition 5. Initially take $\mathfrak{Y}$ to be the class of types given by Proposition 4 (i.e., of all finite abelian groups of order $|G| = p^n$) and take $d = n$. Now survey the $\Lambda_{(p)}$-lattices with this d as in the previous paragraph. Each time a "new" L is found, compute L_G. If this has $\geqslant d$ generators, discard L; otherwise form $\mathfrak{Y}_L$ by adjoining the type of L_G to $\mathfrak{Y}$. Re-define $\mathfrak{Y}$ as $\min \mathfrak{Y}_L$. Moreover, if L happens to be elementary abelian of rank r (necessarily $< d$), re-define d to be r. Now restart the survey with the new $\mathfrak{Y}$ and d. When the survey is complete we have $\mathfrak{Y} = \min \mathfrak{X}_p(G)$ and $d = m(G)$ by Proposition 5.

References

[1] E. Artin, Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz, Hamb. Abh. 7 (1929) 46–51.
[2] K. Gruenberg, A. Weiss, Capitulation and transfer kernels, J. Théor. Nombres Bordeaux 12 (2000) 219–226.
[3] K. Gruenberg, A. Weiss, Capitulation and transfer triples, Proc. London Math. Soc. 87 (2003) 273–290.
[4] S. Iyanaga, Zum Beweis des Hauptidealsatzes, Hamb. Abh. 10 (1934) 349–357.
[5] K. Miyake, The capitulation problem, Sugaku Expositions 1 (1988) 175–194.
[6] I. Reiner, Maximal Orders, London Math. Soc. Monogr. (N.S.), vol. 28, Oxford Univ. Press, New York, 2003.
[7] H. Suzuki, A generalization of Hilbert's Theorem 94, Nagoya Math. J. 121 (1991) 161–169.